Credit Card Procedures

The University accepts credit card payments as a convenience to its customers. University merchants (departments) may accept Visa, MasterCard, or American Express. The Office of the North Carolina State Controller has established a Master Services Agreement (MSA) with SunTrust Merchant Services.

These procedures are designed to protect cardholder data; maximize university compliance with its merchant services provider contract, which includes compliance with the Payment Card Industry Data Standards (PCI DSS) and the various credit card standards; and to ensure appropriate integration with the university’s financial and other systems.

To ensure these standards are adhered to the following procedures are followed:

1. **Credit Card Acceptance Questionnaire**
   
The department requesting to accept credit card payments completes the questionnaire and submits it to the PCI Coordinator. This questionnaire has two purposes: 1) Provides the credit card acceptance committee of the intent and needs of the department; and 2) Apprises the requesting department of the PCI requirements for credit card acceptance. The questionnaire is reviewed by the credit card acceptance committee and in most cases will require review of the PCI committee. Any department approved to accept credit card payments on behalf of the University shall have procedures in place for securely processing, storing and accessing the card holder data environment per the UNCW Credit Card Acceptance Policy and PCI DSS Standards. Yearly training is required.

2. **Departmental Receipting Privileges**
   
The department requests receipting privileges from the controller’s office. These privileges may already exist for departments who deposit payments using other methods. In these cases, the privileges need to be revised to accommodate the receipting method of accepting credit cards.

3. **Determine Credit Card Method**
   
Credit cards may be accepted via Point of Sale (POS) devices or by using a Web application.

- Web applications may require use of a payment gateway (see number 6) and shall adhere to the OSBM Master Services Agreement. Procurement and use of any web application must be reviewed by the PCI Committee. This review is required no matter the merchant involved. PCI documentation will be required from the vendor which may include an Attestation of Compliance (AOC), a responsibility matrix and credit card data mapping.
- POS devices can be purchased or leased through OSC (see number 5). These costs are paid by the department. Once the method is determined, the department indicates this choice on the application for receipting privileges. POS devices will be equipped with TransArmor, a point to point encryption software.
4. Application for Merchant ID
   a) An application for a new merchant ID must be submitted to the Office of State Controller (OSC) by the PCI Coordinator or designee.
   b) Separate merchant numbers are required for Web or POS acceptance methods.
   c) The application process takes 7-10 days. OSC will submit the request to FirstData Merchant Services. Upon completion FirstData will assign a merchant ID (MID), terminal ID (TID), and data ware device ID (DID). These numbers are required for Web application set up with TouchNet and will be programmed into the POS device by FirstData.
   d) The PCI coordinator will notify the requesting department when the application has been completed.
   e) The PCI coordinator will maintain a listing of merchant information for the University by the method of acceptance.

5. Point of Sale (POS) Terminal Purchases
   a) POS terminals are purchased or leased through OSC when requesting a new merchant ID.
   b) TransArmor, an end to end encryption software should also be requested to be loaded on the terminal.
   c) Terminal costs and TransArmor monthly fees are paid by the requesting department.
   d) The requesting department must also ensure a designated data line be installed for the POS terminal.
   e) POS devices shall be stored in a secured location to prevent tampering.
   f) POS terminals should be inspected daily and results of the inspection be logged on the POS inspection form.
   g) POS inspection logs should be turned into the PCI Coordinator or designee monthly.
   h) POS terminals will be inspected yearly by the PCI Coordinator or designee.
   i) An updated listing of POS devices will be maintained by the PCI Coordinator.
   j) POS terminals no longer in use should be turned into the PCI Coordinator for secure storage. The Office of State Controller has instructions on terminal disposal for leased and owned equipment. POS terminals cannot be surplused.

6. TouchNet Setup Procedures - Overview
   a) The TouchNet Administrator meets with the requesting department to discuss their particular need to assess whether an uPay or uStore is needed.
   b) If the department is requesting a software application, then the software vendor has to be included in the TouchNet Ready Partner program (TRP). The TN administrator would contact the TRP program contact to have an addendum to UNCW’s contract created. TouchNet charges both an implementation fee and a yearly fee for UNCW to add a new partner, if the vendor is not already under the current agreement between TouchNet and UNCW. The fees are paid by the requesting department via purchase order. Prior to contracting with any software provider the PCI committee will need to review the providers PCI documentation (Attestation of Compliance, responsibility matrix and data flow diagrams).

   If the vendor is not a part of the TouchNet Ready Partner program, the TouchNet Administrator can work with the vendor, the TRP representative, and the department to discuss the vendor become a part of the program. For vendors unwilling to become TRP, then an uStore would be the recommended. There is no fee associated with using an uStore.
   c) The TouchNet Administrator will work the department to acquire access forms to the TouchNet system.
d) The administrator and the department’s merchant manager will create and test the uStore or uPay site in the test TouchNet Marketplace. A test payment is required.

e) Upon successfully testing, the administrator will create the new uStore or uPay in the production environment. At this point receipting privileges as well as online PCI training (via Skillport) for employees should be completed. Reset of the payment gateway is required. The TouchNet administrator would request this from TouchNet support. A test payment should be performed prior to enabling the site.

f) The TouchNet Administrator will notify the Cashier’s office that the department’s production site is now live.

7. Payment Gateway

TouchNet is currently the primary payment gateway used by University merchants. Use of any other payment gateway must be approved by Associate Vice Chancellor of Finance.

8. Credit Card Deposit & Reconciliation Requirements

   a) Daily reconciliation of credit card charges made by web application or POS is required by the State of North Carolina (G.S. 147-77).

   b) The University merchant (department) must prepare and bring the deposit transmittal with backup documentation to the Cashiers office daily. There should be no discrepancies in the amounts entered on the deposit transmittal compared to the vendor credit card report. Discrepancies must be researched and resolved prior to submitting the deposit to the Cashier’s office.

   c) The University merchant must adhere to the “Instruction’s for Preparing a Deposit Transmittal for Credit Card Transactions” for both Web applications and POS transactions as provided in the finance training course. The deposit transmittal documentation should not include any credit card data. Any credit card information, if written down for phone transactions, should be destroyed after the transaction via shredder. This information should never be included in the deposit transmittal (see section 11 PCI compliance).

   d) Departments receive electronic receipt notification for each deposit transmittal. The department should verify the amounts deposited to the funds and accounts in the general ledger match the amount on the deposit transmittal.

9. Credit Card Fees

University departments (merchants) are responsible for related equipment, supply costs, processing and transaction fees. Processing fees include: interchange fees, assessment and switch fees, merchant service fees. The fee schedule can be found on the North Carolina Office of State Controller’s website. This schedule applies to the Master Services Agreement (MSA) with SunTrust Merchant Services, LLC. Typically, the credit card fees are reconciled to the same funding source as the revenue receipted. Special approval from the credit card acceptance committee is required if the transaction fees do not follow the same as the revenue source.

Appropriated state funds (general funds) cannot used for the credit card transaction fees. Departments may use trust or auxiliary funding provided the revenue source is not derived from student fees.

10. Required Training

   a) RCT201 – Departmental Receipting is required prior to being granted receipting privileges. This course is a part of the Finance Training Program and covers information on deposit transmittal policy and
procedures, credit card policy and procedures and PCI Security compliance requirements (see section 11). Receipting privileges are renewed annually.

b) PCI201 – Data Security Awareness is required for all university employees who may come in contact with credit card data. This course is a part of the Finance Training program and covers the twelve PCI DSS Requirements (see section 11). It is offered online via Skillport and should be renewed annually.

11. Compliance Security of Credit Card Users’ Data

These are the twelve PCI DSS Requirements:

Build and maintain a secure network

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a vulnerability management program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Implement strong access control measures

7. Restrict access to cardholder data by business need to know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to card holder data

Regularly monitor and test networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes (i.e. annual penetration tests which are different than the vulnerability scanning requirement)

Maintain an information security policy

12. Maintain a policy that addresses information security